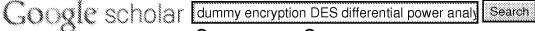
#### Web Images Videos Maps News Shopping Gmail more V



Advanced Scholar Search Scholar Preferences

O Search the Web O Search English pages

## Scholar All articles Recent articles Results 1 - 10 of about 372 for dummy encryption DES differential power analysis. (0.12 seconds)

On boolean and arithmetic masking against differential power analysis - euglaedu.sa (pow

JS Coron, L Goubin - Lecture Notes in Computer Science, 2000 - Springer ... processing can be used by clever attackers to remove dummy code or ... us consider for instance the case of the DES algorithm (Data Encryption Standard). ... Cited by 110 - Related articles - BL Direct - All 17 versions

Securing the AES finalists against power analysis attacks

TS Messerges - Lecture notes in computer science, 2001 - Springer ... [26] look at attacks against the encrypt and decrypt ... at ways to securely implement the AES fundamental operations ... steps such as executing random dummy code or ... Orted by 131 - Related articles - BL Direct - All 5 versions

[PDF] \*... logic with signal independent power consumption to withstand differential power analysis ....

K Tirl, M Akmal, I Verbauwhede - 28th European solid-state circuits conference ( ..., 2002 - Citeseer ... dom process interrupts interleave dummy instructions to ... http:// csrc.nist.gov/encryption/ aes/ round1/conf2 ... and N. Dabbous, "Differential Power Analysis in the ... Oted by 165 - Related articles - All 9 versions

A generic protection against high-order differential power analysis- viagr.org (PDF) ML Akkar, L Goubin - Lecture notes in computer science, 2003 - Springer ... XOR: do it byte per byte, add **dummy** values ... A Generic Protection against High-Order Differential Power Analysis ... and will really slow down the DES execution and ... Cited by 40 - Related articles - BL Direct - All 5 versions

An implementation of DES and AES, secure against some attacks- \*psu.edu (PDF) M Akkar, C Giraud - Lecture notes in computer science, 2001 - Springer ... insertion of dummy instructions; - randomization ... following timings come from the

encryption of a ... Des and differential power analysis, the duplication method. ... Cited by 192 - Related articles - BL Direct - All 7 versions

Masking the energy behavior of DES encryption - \*psuledu (PDF)

H Saputra, N Vijaykrishnan, M Kandemir, MJ ... - Proceedings of the conference on Design, Automation ..., 2003 - portal.acm.org ... key-related data- dependent computations in DES encryption. ... technique involves adding dummy modules and ... Differential power analysis (DPA) is currently the most ... Cited by 43 - Related articles - All 19 versions

Multiplicative masking and power analysis of AES- • oregonstate.edu (Por)

JD Golic, C Tymen - Lecture notes in computer science, 2003 - Springer ... and randomize elementary computations involving the secret key, eg, by randomly introducing dummy operations and ... 201 2 Differential Power Analysis of AES ... Cited by 96 - Related articles - BL Direct - All 16 versions

## Power analysis, what is now possible

ML Akkar, R Bevan, P Dischamp, D Moyart - Lecture Notes in Computer Science, 2000 - Springer ... 3.2 PODPA (Perhaps Optimal Differential Power Analysis) ... (ie AES candidates, RSA ... of the key with- out modifying the algorithm used or using multiple encryption. ... O4ed by 84 - Related articles - BL Direct - All 4 versions

dummy encryption DES differential power analysis - Google Scholar

#### A collision-attack on AES combining side channel-and differential-attack- •num-uni-boohum.de (Port

K Schramm, G Leander, P Felke, C Paar - Cryptographic Hardware and Embedded Systems--CHES ..., 2004 - books.google.com ... such as random wait states or dummy cycles will ... of averagings per encryption) are required to detect ... DES and differential power analysis: the dupli -cation ...

Clied by 36 - Related articles - BL Direct - All 8 versions

### Simplified adaptive multiplicative masking for AES- \*ugu.edu.sa (PDF)

E Trichina, D De Seta, L Germani - Lecture Notes in Computer Science, 2003 - Springer

... box of the first round of the Advanced Encryption Standard (AES) [6] will ... ran- dom

timing shifts and wait states, inserting dummy instructions, random ...

Cited by 65 - Related articles - BL Direct - All 6 versions

# Goolooooogle ≫ 1 2 3 4 5 6 7 8 9 10 Next

Result Page:

dummy encryption DES differential Search

Go to Google Home - About Google - About Google Scholar

©2009 Google